

Rhonda M. Bolton
202.429.6495
rbolton@step toe.com

April 28, 2003

Via ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, SW – Room TW-A325
Washington, D.C. 20554

Re: *Ex Parte* Presentation -- *In the Matter of Digital Broadcast Copy Protection*,
MB Docket No. 02-230

Dear Ms. Dortch:

In accordance with Section 1.1206 of the Commission's Rules, 47 C.F.R. § 1.1206, Veridian Corporation ("Veridian"), through its undersigned counsel, writes to notify the Commission of an *ex parte* presentation in the above-referenced docket. On April 25, 2003, representatives of Veridian met with Jordan Goldstein, Senior Legal Advisor to Commissioner Copps.

In the meeting, Veridian's representatives emphasized the need for further Commission proceedings to set standards allowing a number of effective digital copy protection methodologies to compete in the marketplace. The Commission should accomplish this through the vehicle of a formal or informal negotiated rulemaking, which is very well suited to the questions in dispute in this proceeding. The representatives of Veridian also discussed the disadvantages of the broadcast flag regime proposed by certain parties to this proceeding and corresponding advantages of source encryption technologies.

The attached slide presentation describes in more detail the matters addressed in the meeting.

Ms. Marlene H. Dortch
April 28, 2003
Page 2

This *Ex Parte* Notice is being filed electronically as permitted by Section 1.1206 (b)(2) of the Commission's Rules.

Respectfully submitted,

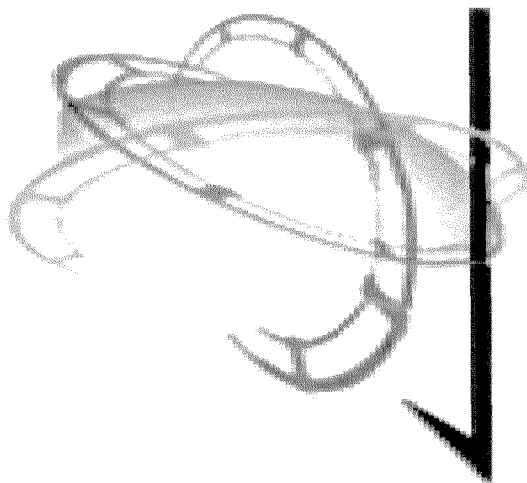
A handwritten signature in black ink, appearing to read "Rhonda M. Bolton". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Rhonda M. Bolton
Counsel for Veridian Corporation

Attachment

cc: Mr. Jordan Goldstein

***Ex Parte* Presentation Regarding Digital Television Copy Protection**



**Veridian Corporation
April 25, 2003**

VERIDIAN

SUMMARY

- The Commission should not impose broadcast flag requirements, which would be costly, ineffective and inflexible and may not be within Commission jurisdiction
- “Source encryption” methodologies are both less costly and more effective
- The Commission should not prescribe any particular technology but can and should prescribe standards to let the market work and promote the public interest
- A negotiated rulemaking or similar informal process is the best way to proceed

Factors to Consider in Cost-Benefit Analysis of Broadcast Flag

- **Costs are High –**
 - **Universal implementation necessary**
 - **All “Downstream” Devices (e.g., PCs) Must Also Incorporate Flag to Access Digital Broadcast Content, Threatening Desired Convergence of PC and TV set**
- **Benefits are Low –**
 - **Weak Form of Protection –**
 - **Legacy or pirated devices without the circuitry can compromise the protection system**
 - **Will ultimately leave content providers as reluctant to license their content as before**
 - **Intrusive –**
 - **May deprive consumers of ability to “space shift” content beyond network where copy is made**
- **Commission Jurisdiction to Mandate Flag is Questionable –**
 - **No explicit authority in Communications Act**
 - **Implicit authority in either Title I or Title III of the Act Doubtful**

Factors to Consider in Cost-Benefit Analysis of Source Encryption

- **Cost effective –**
 - Universal adoption not necessary to protect premium content likely to be most closely guarded by owners
 - Per unit implementation cost expected to be same or less than broadcast flag
- **Greater Benefits –**
 - Higher level of protection
 - Source encryption system not compromised by devices that lack encryption circuitry
 - More flexible protection better accommodates the public interest
 - Does not prohibit “space shifting;” a consumer may view protected content if the consumer has the appropriate “ticket”
 - Allows content owners to place situational parameters on access to protected content, e.g., start and end viewing dates, resolution, maximum screen size, multichannel sound, and future enhancements
- **Source encryption of ancillary and supplementary DTV services clearly within Commission’s jurisdiction, 47 U.S.C. § 336 (a)(2)**

What Commission Involvement Should Not, and What It Can, Achieve

- Should Not Pick Winners
- Can:
 - Develop record concerning need for DTV copy protection
 - Facilitate development of standards that will allow marketplace to choose acceptable technology
 - Develop standards that will achieve balance between consumers' interests and those of content providers

Ideal Circumstances for Negotiated Rulemaking¹

- Topic is “new”
- Agency is considering standards
- Issues sufficiently crystallized to make an exchange of ideas useful
- Parties’ positions not yet “hardened”
- Large investments not yet made

¹ See, e.g., 1 Charles Koch, Administrative Law Treatise §4.36; Phillip Harter, Negotiating Regulations: A Cure for Malaise, 71 Geo. L.J. 1 (1982).

DTV Copy Protection Issue Is Well-Suited for Negotiated Rulemaking

1. DTV copy protection issue relatively new
2. Copy protection standards are under consideration
3. Issues sufficiently crystallized – many commenters agree that some type of DTV copy protection standard will be necessary
4. Parties' positions do not appear to be hardened – no large investments have been made in any particular technology

Issues The Negotiated Rulemaking Committee Should Consider:

- **The Effectiveness (including a cost-benefit analysis) and Appropriateness of the Broadcast Flag technology;**
- **The Effectiveness (including a cost-benefit analysis) and Appropriateness of the Source-encryption-based technologies**
- **Standards That Must Be Satisfied by Any Accepted Technology or Implementation Method**
- **The Interaction Between the Questions Raised here and Digital Copy Protection for MVPD's (e.g., "plug and play" standards)**

Appropriate Minimum Standards for a DTV Copy Protection System

1. Robustness
and reliability
2. Openness
3. Visibility
4. Renewability
5. Compatibility

Appropriate Minimum Standards for a DTV Copy Protection System

1. Minimum standard for
robustness and reliability –

No “shared secrets”



Appropriate Minimum Standards for a DTV Copy Protection System

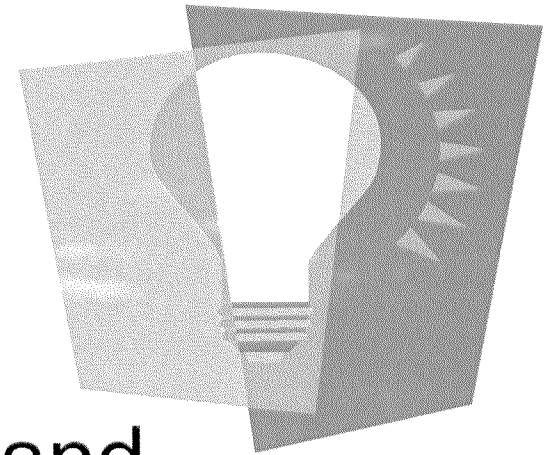
2. Openness –



The method must be open to all consumer equipment manufacturers, distribution platforms, and all content providers indiscriminately

Appropriate Minimum Standards for a DTV Copy Protection System

3. Visibility –



The algorithms, specifications, and parameters of the method must be open to consumers. *The efficacy of the system should not be compromised by such visibility.*

Appropriate Minimum Standards for a DTV Copy Protection System

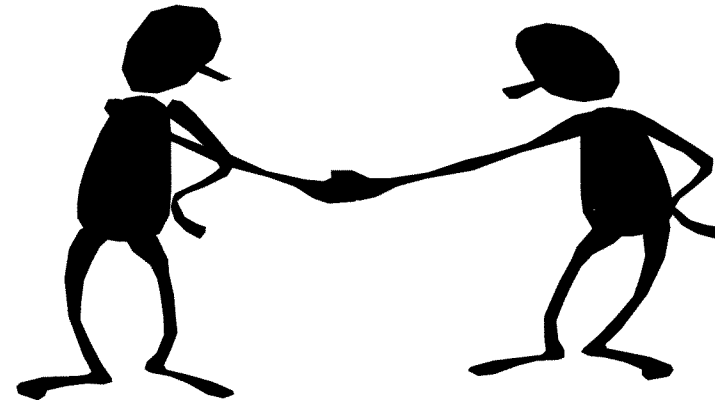
4. Renewability –



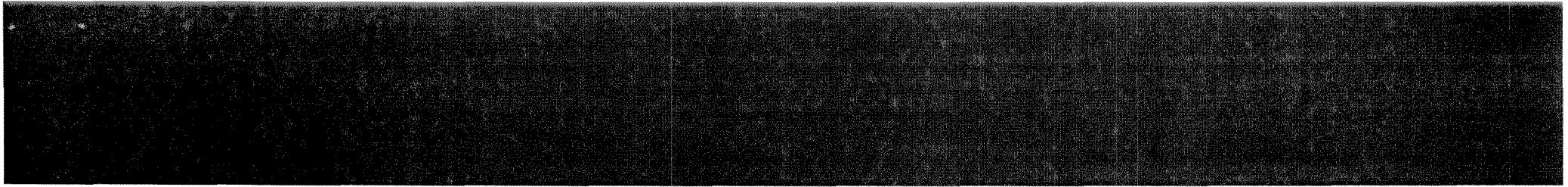
If compromised, the system must be capable of recovering and continuing to protect content *without a total recall or invalidation of all installed consumer equipment.*

Appropriate Minimum Standards for a DTV Copy Protection System

5. Compatibility –



- The method must not preclude use of a different, competing method, and
- The method must allow next-generation techniques to be deployed with minimal conversion requirements



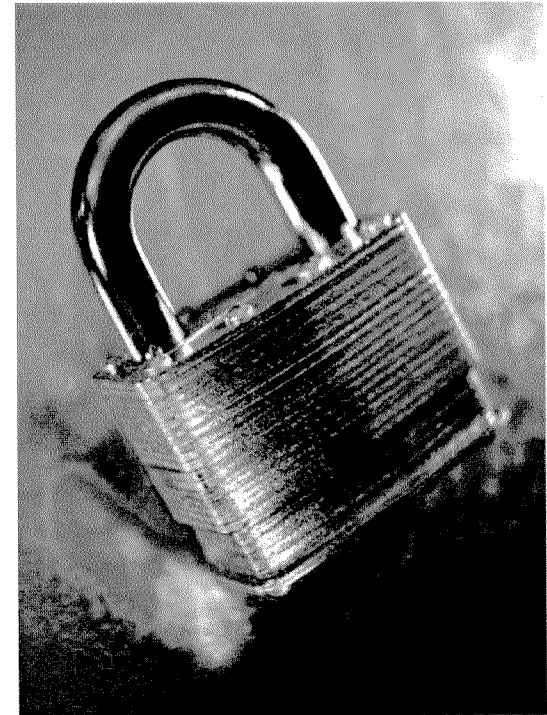
The Commission Can Facilitate
Development of Standards
Expeditiously and Efficiently
Through

Negotiated Rulemaking

Source Encryption – A Better DTV Copy Protection Alternative

“Persistent Access Control” such
as VeriFIDES™ –

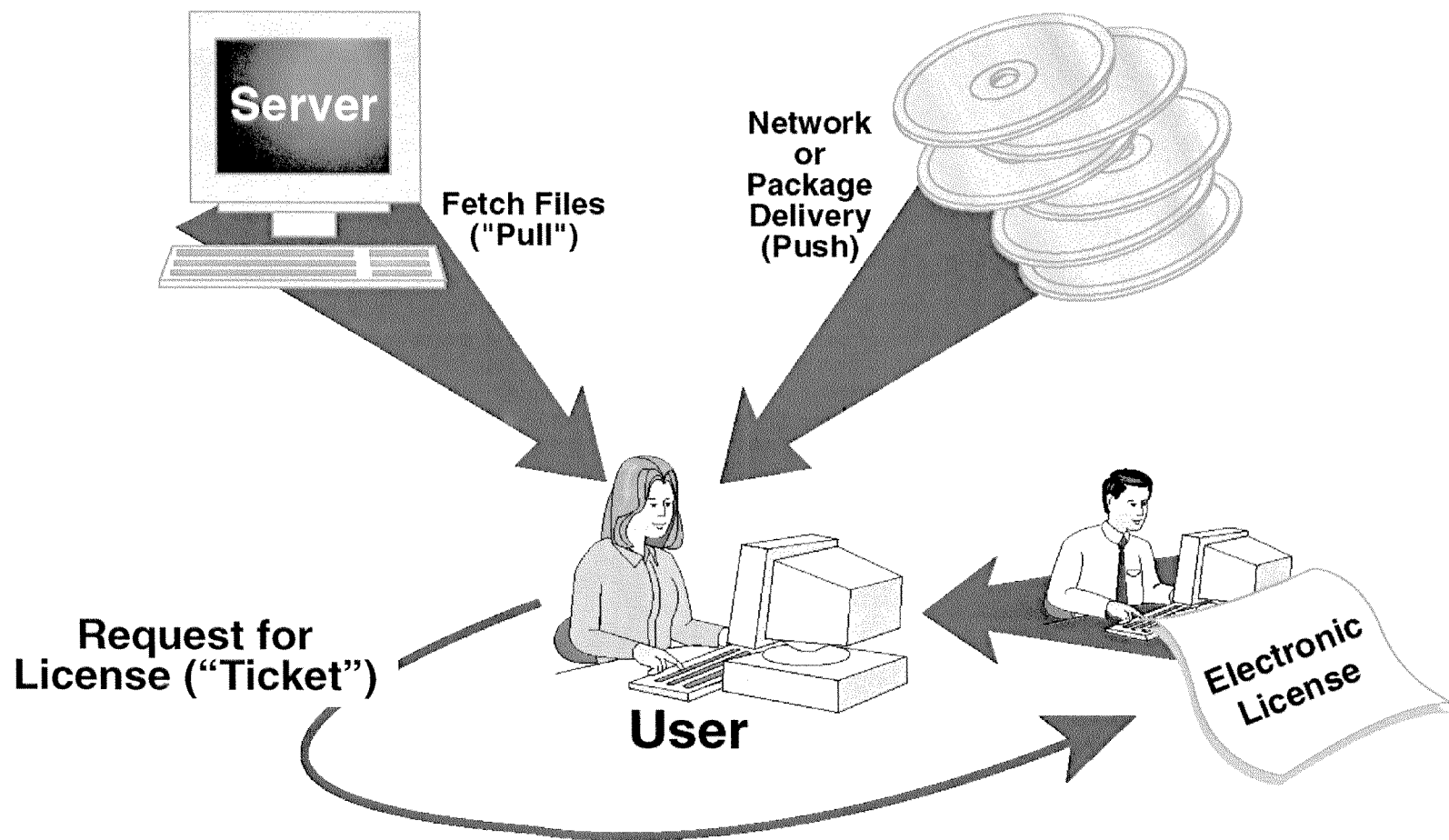
Technology that Prevents Piracy



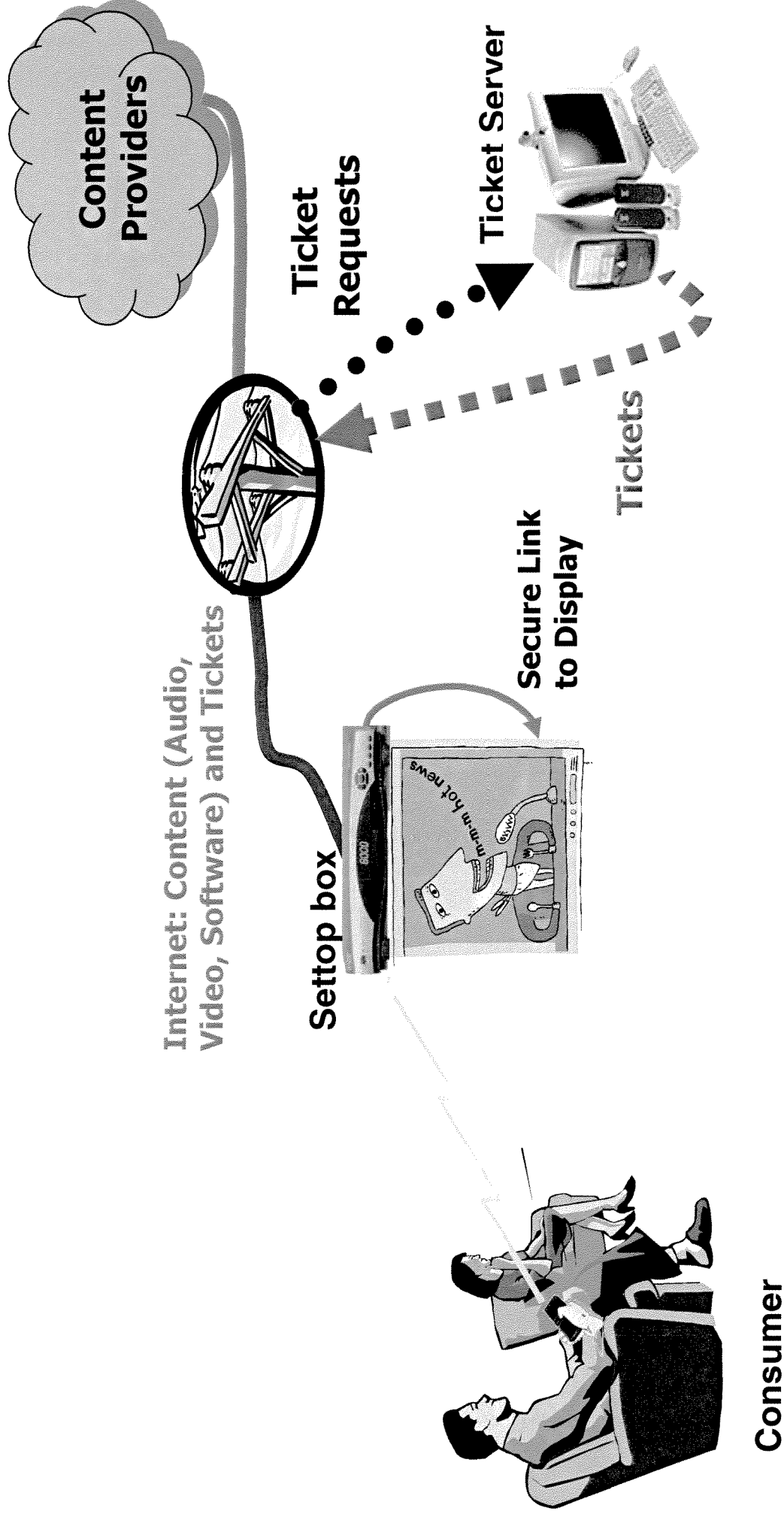
Operational Concept

Repository of Protected Files

Broadcast of Protected Files



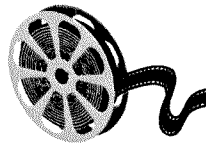
What it is, in pictures



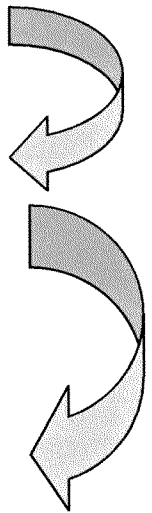
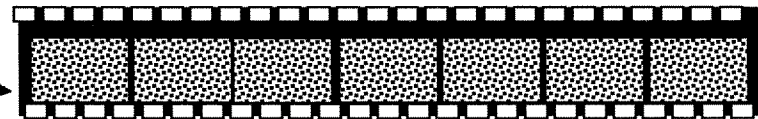
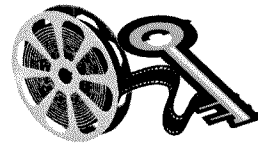
How it works – Step 1: Secret Key encryption

Content Packaging

Original Program
(*Murder on the Occidental Local*)



Encrypted Program
By the Secret Key

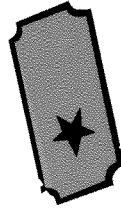
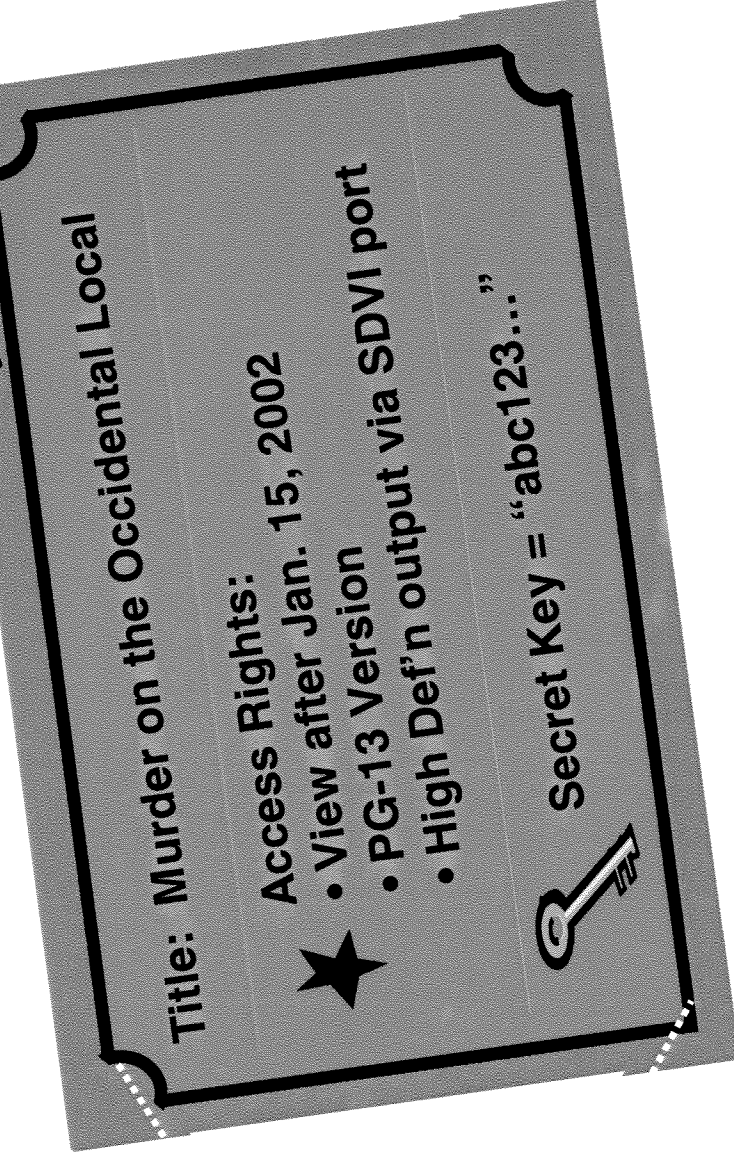


Title: Murder on the Occidental Local	
<div>Encrypted (by Secret Key) Content</div>	To: J. User From: Content Owner

Once encrypted with the secret key, content can be sent like a postcard (open to all)

How it works – Step 2: Create the ticket

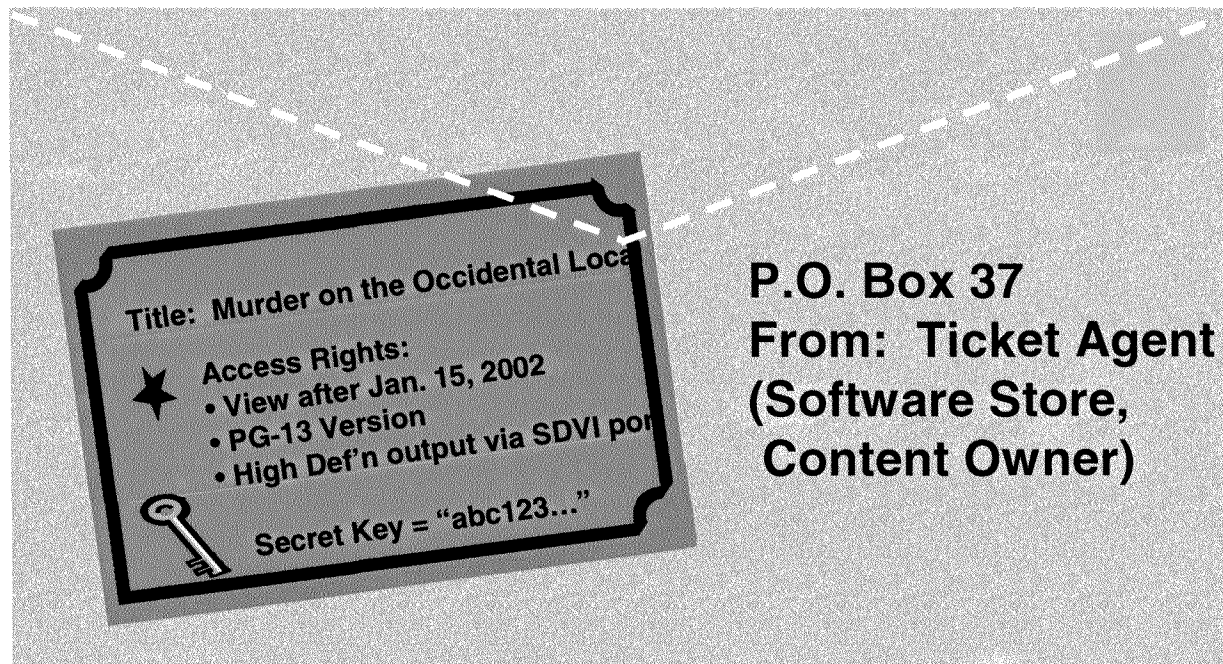
Ticket (Public Key  Encrypted)



How it works – Step 3: Encrypt the ticket with user's Public Key and send it

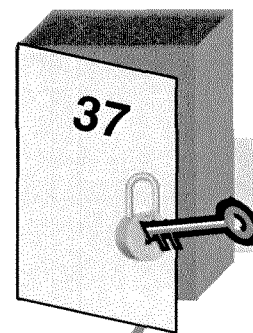
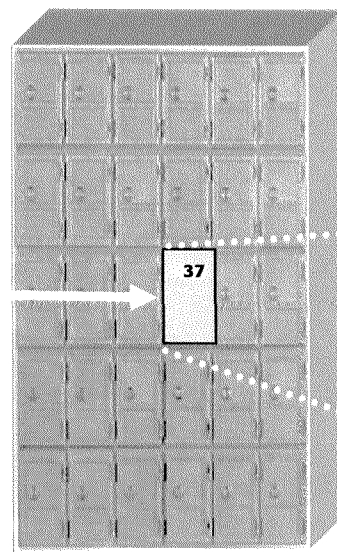
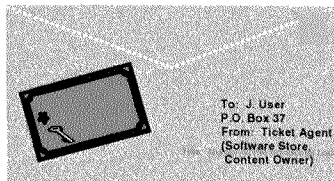
Once encrypted with the public key, the ticket is like a first-class letter sent to a PO Box– available only to the addressee with his “unique” private key.

Public Key  Encryption

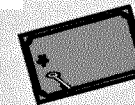


How it works – Step 4: Allow access to the user, as authorized by the ticket

**Ticket - Sent
directly to
customer***



Ticket



Content



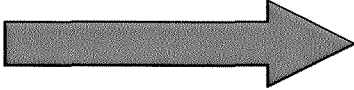
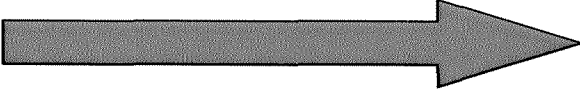
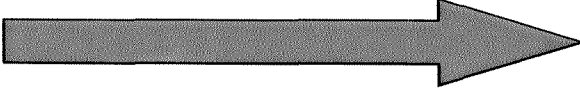
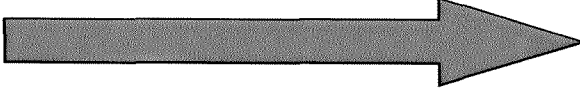
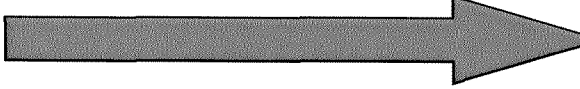
*** Only the customer's unique Private Key for box 37 can retrieve the contents of the ticket.**

Characteristics

- **Secure: Protects high value content from piracy**
- **Enables 'fair use' as expected by consumers**
- **Open; protects privacy; allows anonymity**
- **Renewable**
 - **Individual devices (or models) can be excluded**
 - **"Go Forward" scenario in event of compromise**
- **Scalable**
 - **No clearinghouse required for each transaction**
 - **Offline operation: full-time connection not required**
- **Compatible with and extensible to PCs**

VeriFIDES™ Meets and Exceeds The Appropriate Minimum Standards for a Copy Protection System –

VeriFIDES™

- Robustness, reliability**  No “Shared Secrets”
- Openness**  Open to all consumer equipment manufacturers, distribution platforms and content providers
- Visibility**  Algorithms, parameters and specs open to consumers
- Renewability**  If compromised, can protect future content without total recall of all installed consumer equipment
- Compatibility**  Does not preclude use of different methods and allows deployment of next-generation methods

***Ex Parte* Presentation Regarding Digital Television Copy Protection**



Veridian Corporation
April 25, 2003